Polytechnique 1998 Deuxième composition de Mathématiques
Option MP

Première partie.

1.a) Si $\dim_{\mathbb{K}}(\mathbb{K}[\alpha]) \leq n < +\infty$, alors la famille $(1, \alpha, \quad , \alpha^n)$ est liée ($n+1$ éléments)
donc il existe $(a_0, \dots, a_n) \neq (0, \dots, 0)$ dans $\mathbb{K}^{n+1}$
tel que $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$.
le polynôme $P = a_0 + a_1 X + \dots + a_n X^n$ est donc un élément non nul de $I_{\mathbb{K}}(\alpha)$.
On a donc prouvé (i) => (ii).
Réciproquement, supposons $I_{\mathbb{K}}(\alpha) \neq \{0\}$ il existe alors $P = a_0 + a_1 X + \dots + a_n X^n$ non nul tel que $P(\alpha)$.
Soit β dans $\mathbb{K}[\alpha]$ $\exists d \in \mathbb{N}$ $(b_0, \quad , b_d) \in \mathbb{K}^{d+1}$ tel que
$\beta = b_0 + b_1\alpha + \dots + b_d\alpha^d = Q(\alpha)$ avec $Q = b_0 + b_1 X + \dots + b_d X^d$.
On effectue la division euclidienne de Q par P.
$Q = PR + S$ avec $\deg S < n$.
On a $\beta = Q(\alpha) = P(\alpha)R(\alpha) + S(\alpha) = S(\alpha) = \sum_{k=0}^{n-1} c_k \alpha^k$
Donc $\mathbb{K}[\alpha] \subset \mathrm{Vect}\{1, \alpha, \quad , \alpha^{n-1}\} (\subset \mathbb{K}[\alpha])$
et par conséquent $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < n-1$.
On a prouvé (ii) => (i)

I.b) $\begin{cases} - 0 \in I_{\mathbb{K}}(\alpha) \\ - \forall (P, Q) \in I_{\mathbb{K}}(\alpha) \quad P(\alpha) - Q(\alpha) = 0 \quad \text{donc } P - Q \in I_{\mathbb{K}}(\alpha) \\ - \forall P \in I_{\mathbb{K}}(\alpha), \ \forall Q \in \mathbb{K}[X] \ (PQ)(\alpha) = P(\alpha)Q(\alpha) = 0 \text{ donc } PQ \in I_{\mathbb{K}}(\alpha) \end{cases}$

Il résulte de ces trois propriétés que $I_{\mathbb{K}}(\alpha)$ est un idéal de $\mathbb{K}[X]$, non réduit à $\{0\}$ car α est algébrique. On sait alors qu'il est engendré par un unique polynôme unitaire P.

$I_{\mathbb{K}}(\alpha) = P\,\mathbb{K}[X]$. ②

P est irréductible, en effet sinon $P = P_1 P_2$ avec $P_1 \neq 0$ $P_2 \neq 0$, et $\deg P_1 < \deg P$ $\deg P_2 < \deg P$ or $P(\alpha) = 0$ donc $P_1(\alpha) P_2(\alpha) = 0$. Donc $P_1(\alpha) = 0$ (par exemple) et par conséquent $P_1 \in I_{\mathbb{K}}(\alpha)$ donc $P \mid P_1$, mais $P_1 \neq 0$ donc $\deg P_1 \geqslant \deg P$. Il y a une contradiction. PS : le raisonnement précédent ne s'applique pas à 1 qui n'est pas irréductible. Mais 1 n'annule aucun α, donc $P \neq 1$.

1.c) L'argument utilisé en 1.a) pour prouver (ii) $\Rightarrow$ (i) prouve que $\dim \mathbb{K}[\alpha] \leqslant \deg P = d$

De plus la famille $(1, \alpha, \ldots, \alpha^{d-1})$ est libre car sinon il existerait un polynôme R non nul de degré $< d$ tel que $R(\alpha) = 0$ (ce qui est impossible, argument vu en 1.b)). Donc $\dim \mathbb{K}[\alpha] \geqslant d$ et finalement $\dim \mathbb{K}[\alpha] = \deg P$

1.d) Soit β un élément non nul de $\mathbb{K}[\alpha]$, on peut écrire $\beta = b_0 + b_1\alpha + \ldots + b_{d-1}\alpha^{d-1} = R(\alpha)$, avec $R \neq 0$ et $\deg R < \deg P$.

Puisque P est irréductible R et P sont premiers entre eux. D'après le théorème de Bézout il existe donc U et V dans $\mathbb{K}[X]$ tels que

$$UR + VP = 1.$$

On en déduit $U(\alpha) R(\alpha) + \underbrace{V(\alpha) P(\alpha)}_{=0} = 1$

donc $U(\alpha)$ est un inverse dans $\mathbb{K}[\alpha]$ de β

Tout élément non nul de l'anneau $\mathbb{K}[\alpha]$ est inversible donc $\mathbb{K}[\alpha]$ est un corps.

PS L'énoncé ne dit pas que $\mathbb{K}[\alpha]$ est un sous-anneau de $\mathbb{C}$
Il est néanmoins facile de vérifier que 1 est dans $\mathbb{K}[\alpha]$
et que $\mathbb{K}[\alpha]$ est stable pour le produit.

2a) $\sqrt{2}$ est annulé par X^2-2, donc le polynôme minimal de $\sqrt{2}=\alpha$ divise X^2-2.

Si X^2-2 n'était pas irréductible ~~sur~~ dans $\mathbb{Q}[X]$ il posséderait un facteur de degré 1. Il existerait donc $\frac{p}{q}$ dans $\mathbb{Q}$ avec $p \wedge q = 1$ et $\frac{p^2}{q^2} = 2$.

Or $\frac{p^2}{q^2} - 2 = 0$

$$\begin{aligned}
&\Rightarrow p^2 = 2q^2 \\
&\Rightarrow 2 \mid p^2 \text{ et } p^2 = 2q^2 \\
&\Rightarrow 2 \mid p \text{ et } p^2 = 2q^2 \quad \text{(car 2 est premier donc } 2 \mid ab \Rightarrow 2 \mid a \text{ ou } 2 \mid b) \\
&\Rightarrow p = 2p' \text{ et } 4p'^2 = 2q^2 \\
&\Rightarrow p = 2p' \text{ et } 2p'^2 = q^2 \\
&\Rightarrow p = 2p' \text{ et } q = 2q' \quad \text{(raisonnement symétrique)}
\end{aligned}$$

$\frac{p^2}{q^2} - 2 = 0 \Rightarrow p \wedge q \geq 2$ Contradiction.

2b) $\alpha^2 = \frac{1+\sqrt{5}}{2} = \beta$ et $\beta^2 - \beta - 1 = 0$ donc

$P = X^4 - X^2 - 1$ est un polynôme annulateur de α.

P est irréductible.

- Il ne possède pas de facteur de degré 1, sinon il posséderait une racine rationnelle $\frac{p}{q}$ avec $p \wedge q = 1$.
  On aurait $p^4 - p^2q^2 - q^2 = 0$ donc $q \mid p^4$ or $q \wedge p^4 = 1$ d'après le théorème de Gauss donc $q \mid p^4 \Rightarrow q = \pm 1$, un raisonnement similaire donne $p = \pm 1$ donc finalement $\frac{p}{q} = \pm 1$, or ni 1 ni -1 n'est racine de P.
- Si P se factorise en un produit de deux polynômes du deuxième degré, que l'on peut supposer unitaires, alors
  $P = (X^2 + aX + b)(X^2 + cX + d)$
  l'examen du coefficient de X^3 donne $c = -a$, ensuite celui de X donne $a(d-b) = 0$ c'est à dire $a = 0$ et dans ce cas on doit avoir ~~$b+d=-1$~~ ~~$bd=-1$~~ $-b$ est racine rationnelle de $X^2 - X - 1$. Le raisonnement précédent montre que c'est impossible; ou bien $b = d$ ce qui contredit $bd = -1$.

$P = X^4 - X^2 - 1$ est irréductible et annule α, c'est son polynôme minimal.

Deuxième partie.

3) Si P est irréductible, alors $\deg P \geq 1$ donc $P' \neq 0$ et $\deg P' < \deg P$. Donc P et P' sont premiers entre eux.
Il existe $(U, V) \in \mathbb{K}[X]^2$ $UP + VP' = 1$.
Si $P(\alpha) = 0$ alors $U(\alpha)P(\alpha) + V(\alpha)P'(\alpha) = 1$, soit $V(\alpha)P'(\alpha) = 0$ en particulier $P'(\alpha) \neq 0$. les zéros complexes de P sont donc simples. ~~tous~~

4.a) On a vu que tout élément de $\mathbb{K}[\alpha]$ s'écrit ~~sous~~ la forme $Q(\alpha)$. Définissons

$$\sigma_i : \mathbb{K}[\alpha] \to \mathbb{C}$$
$$Q(\alpha) \mapsto Q(\lambda_i)$$

Il faut prouver que σ_i est bien définie.
Or si $Q_1(\alpha) = Q_2(\alpha)$ alors $(Q_1 - Q_2)(\alpha) = 0$ donc $P_{\mathbb{K}}(\alpha)$ divise $Q_1 - Q_2$ et $Q_1 - Q_2 = Q_3 P_{\mathbb{K}}(\alpha)$.
On en déduit $Q_1(\lambda_i) - Q_2(\lambda_i) = Q_3(\lambda_i) \underbrace{P_{\mathbb{K}}(\alpha)(\lambda_i)}_{=0} = 0$
et on a bien $Q_1(\alpha) = Q_2(\alpha) \Rightarrow Q_1(\lambda_i) = Q_2(\lambda_i)$ donc σ_i est bien défini.
Il est immédiat que σ_i est un morphisme d'algèbre
($\sigma_i(P(\alpha) + Q(\alpha)) = \sigma_i(P(\alpha)) + \sigma_i(Q(\alpha))$ donc $\sigma_i(\beta + \gamma) = \sigma_i(\beta) + \sigma_i(\gamma)$
et de même $\sigma_i(1) = 1$ $\sigma_i(\beta\gamma) = \sigma_i(\beta)\sigma_i(\gamma)$)
Si $\tilde{\sigma}_i$ est un morphisme d'algèbre tel que $\tilde{\sigma}_i(\alpha) = \lambda_i$
alors pour tout polynôme $\tilde{\sigma}_i(P(\alpha)) = P(\tilde{\sigma}_i(\alpha)) = P(\lambda_i)$
ce qui prouve $\tilde{\sigma}_i = \sigma_i$ et l'unicité de σ_i

4.b) Si σ un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$
on a $\sigma(\underbrace{P_{\mathbb{K}}(\alpha)(\alpha)}_{=0}) = P_{\mathbb{K}}(\alpha)(\sigma(\alpha))$

$$0 = P_{\mathbb{K}}(\alpha)(\sigma(\alpha))$$

donc il existe un i tel que $\sigma(\alpha) = \lambda_i$ et $\sigma = \sigma_i$
On obtient bien ainsi tous les morphismes de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ vers $\mathbb{C}$. Il en existe n car les racines complexes de $P_{\mathbb{K}}(\alpha)$ sont simples.

5) - $\beta \in \mathbb{K}[\alpha]$ et $\mathbb{K}[\alpha]$ est une sous-algèbre donc $\mathbb{K}[\beta] \subset \mathbb{K}[\alpha]$. En particulier $\mathbb{K}[\beta]$ est un sous-espace vectoriel de $\mathbb{K}[\alpha]$ et $\dim_{\mathbb{K}} \mathbb{K}[\beta] \leq \dim_{\mathbb{K}} \mathbb{K}[\alpha]$.

- Soit $P_{\mathbb{K}}(\beta)$ le polynôme minimal de β (qui existe car $\dim_{\mathbb{K}} \mathbb{K}[\beta] < +\infty$).

Or a $P_{\mathbb{K}}(\beta) = 0$, donc puisque les σ_i sont des morphismes de $\mathbb{K}$-algèbres !

$$\forall i \quad P_{\mathbb{K}}(\beta)(\sigma_i(\beta)) = \sigma_i(P_{\mathbb{K}}(\beta)(\beta)) = 0$$

Donc $P_{\mathbb{K}}(\beta)$ possède au moins n racines distinctes

donc $\dim \mathbb{K}[\beta] = \deg P_{\mathbb{K}}(\beta) \geqslant n = \dim \mathbb{K}[\alpha]$

- En récapitulant $\mathbb{K}[\beta] \subset \mathbb{K}[\alpha]$ et $\dim_{\mathbb{K}} \mathbb{K}[\beta] = \dim_{\mathbb{K}} \mathbb{K}[\alpha]$

donc $\mathbb{K}[\beta] = \mathbb{K}[\alpha]$

6) Pour tout couple i, j, avec $i \neq j$, $\sigma_i(\alpha) \neq \sigma_j(\alpha)$.

Donc si $i \neq j$ et $\sigma_i(\beta) = \sigma_j(\beta)$ $\forall \lambda \in \mathbb{K}$ $\sigma_i(\alpha + \lambda\beta) = \sigma_i(\alpha) + \lambda\sigma_i(\beta) \neq \sigma_j(\alpha + \lambda\beta)$

et si $\sigma_i(\beta) \neq \sigma_j(\beta)$ $\sigma_i(\alpha + \lambda\beta) = \sigma_j(\alpha + \lambda\beta) \iff \lambda = \dfrac{\sigma_i(\alpha) - \sigma_j(\alpha)}{\sigma_j(\beta) - \sigma_i(\beta)}$.

Il n'y a donc qu'un nombre fini de λ dans $\mathbb{K}$ pour lesquels il existe un couple (i, j) avec $i \neq j$ et $\sigma_i(\alpha + \lambda\beta) = \sigma_j(\alpha + \lambda\beta)$.

Or $\mathbb{K}$ est un sous-corps de ~~$\mathbb{K}$~~ $\mathbb{C}$, il contient donc au moins $\mathbb{Q}$ et en particulier il est infini.

Il existe donc au moins λ_1 et λ_2 distincts, dans $\mathbb{K}$ et tels que : $\forall i, j$ $i \neq j$ $\sigma_i(\alpha + \lambda_1\beta) \neq \sigma_j(\alpha + \lambda_1\beta)$, $\sigma_i(\alpha + \lambda_2\beta) \neq \sigma_j(\alpha + \lambda_2\beta)$

Prenons $\beta_1 = \dfrac{\alpha + \lambda_1\beta}{\lambda_1 - \lambda_2}$ $\quad \beta_2 = \dfrac{\alpha + \lambda_2\beta}{\lambda_2 - \lambda_1}$.

Or si $i \neq j$ $\sigma_i(\beta_1) = \dfrac{1}{\lambda_1 - \lambda_2}\sigma_i(\alpha + \lambda_1\beta) \neq \sigma_j(\beta_1)$ et de même $\sigma_i(\beta_2) \neq \sigma_j(\beta_2)$

Donc $\mathbb{K}[\beta_1] = \mathbb{K}[\alpha]$ $\mathbb{K}[\beta_2] = \mathbb{K}[\alpha]$ et $\beta = \beta_1 + \beta_2$.

Troisième partie.

7) $\mathbb{Q}[\alpha]$ est corps (question 1.d) contenu dans K. K est donc bien un espace vectoriel sur $\mathbb{Q}[\alpha]$. Si $(x_1, \quad, x_m)$ est une famille $\mathbb{Q}[\alpha]$-libre d'éléments de K elle est aussi $\mathbb{Q}$-libre car $\mathbb{Q} \subset \mathbb{Q}[\alpha]$. Donc $m \leq \dim_{\mathbb{Q}}(K)$. Toute famille $\mathbb{Q}[\alpha]$-libre d'éléments de K possède au plus $\dim_{\mathbb{Q}}(K)$ éléments. K est donc un $\mathbb{Q}[\alpha]$-espace vectoriel de dimension finie et $\dim_{\mathbb{Q}[\alpha]} K \leq \dim_{\mathbb{Q}} K$. Ceci justifie l'existence de d et de la base $(e_1, \quad, e_d)$.

Soit x dans K. On peut écrire $x = \sum_{i=1}^{d} x_i e_i$ où chaque x_i est dans $\mathbb{Q}[\alpha]$ et peut donc s'écrire $x_i = \sum_{j=0}^{m-1} a_{i,j} \alpha^j$, $a_{i,j} \in \mathbb{Q}$.

x peut donc s'écrire $\sum_{i=1}^{d} \sum_{j=0}^{m-1} a_{i,j} \alpha^j e_i$, $a_{i,j} \in \mathbb{Q}$. La famille $(\alpha^j e_i)_{1 \leq i \leq d, 0 \leq j \leq m-1}$ est donc une famille $\mathbb{Q}$-génératrice de K

Si $\sum_{i=1}^{d} \sum_{j=0}^{m-1} a_{i,j} \alpha^j e_i = 0$ alors $\sum_{i=1}^{d} \underbrace{\left(\sum_{j=0}^{m-1} a_{i,j} \alpha^j\right)}_{x_i} e_i = 0$

$\forall i$ $x_i \in \mathbb{Q}(\alpha)$ et $(e_1, \quad, e_d)$ est libre, donc $\forall i$ $x_i = 0$

ensuite $\forall i$ $\sum_{j=0} a_{i,j} \alpha^j = 0$ et $a_{i,j} \in \mathbb{Q}$ et $(1, \quad \alpha^{m-1})$ est libre

donc $\forall i, j$ $a_{i,j} = 0$.

La famille $(\alpha^j e_i)_{1 \leq i \leq d, 0 \leq j \leq m-1}$ est donc $\mathbb{Q}$-libre.

Finalement cette famille est une $\mathbb{Q}$-base de K et on obtient

$$\dim_{\mathbb{Q}} K = \dim_{\mathbb{Q}[\alpha]} K \times \dim_{\mathbb{Q}} \mathbb{Q}[\alpha].$$

8a) Ordonnons clairement la base de la question précédente (7)

en $\mathcal{B} = (e_1, \alpha e_1, \dots, \alpha^{m-1} e_1, e_2, \alpha e_2, \dots, \alpha^{m-1} e_2, \dots, e_d, \dots, \alpha^{m-1} e_d)$

Si $0 \leq j < m-1$ $\quad \alpha.(\alpha^j e_i) = \alpha^{j+1} e_i$

$j = m-1$ $\quad \alpha(\alpha^{m-1} e_i) = \alpha^m e_i = \left(-\sum_{k=0}^{m-1} a_k \alpha^k\right) e_i$

si $P_{\mathbb{Q}}(\alpha) = X^m + \sum_{k=0}^{m-1} a_k X^k$.

La matrice de M_α dans la base $\mathcal{B}$ est donc une matrice diagonale par blocs $M = \begin{pmatrix} C & & 0 \\ 0 & C & \\ & & 0 \\ 0 & 0 & C \end{pmatrix}$ où C est

la matrice compagnon $\begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & \vdots & -a_1 \\ 0 & & & \\ \vdots & \ddots & 0 & \\ 0 & \cdots\ 0 & 1 & -a_{m-1} \end{pmatrix}$, donc.

$\Delta_\alpha = (\Delta_C)^d$ avec $\Delta_C = \det(XI_m - C) = \begin{vmatrix} X & & a_0 \\ -1 & & a_1 \\ & & \\ & -1 & X+a_{m-1} \end{vmatrix}$

Pour calculer Δ_C on effectue l'opération sur les lignes $L_1 \leftarrow L_1 + XL_2 + \quad + X^{m-1} L_m$, puis on développe par rapport à la première ligne dont seul le dernier coefficient est maintenant non nul.

$$\Delta_C = (-1)^{m+1} \underbrace{(a_0 + a_1 X + \quad + a_{m-1} X^{m-1} + X^m)}_{P_{\mathbb{Q}}(\alpha)} \times \underbrace{\begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & & & & 0 \\ & & & & X \\ 0 & \cdots & & 0 & -1 \end{vmatrix}}_{(-1)^{m-1}}$$

Donc $\Delta_C = P_{\mathbb{Q}}(\alpha)$ et $\Delta_\alpha = (P_{\mathbb{Q}}(\alpha))^d$

8.b) $Tr(M_\alpha) = d\, Tr(C) = -d\, a_{m-1} = d\left(\sum_{i=1}^m \alpha_i\right)$ où les α_i sont des racines (distinctes de $P_{\mathbb{Q}}(\alpha)$). Si on remarque maintenant qu'on peut écrire $\alpha = \beta_1 + \beta_2$ avec $\mathbb{Q}[\beta_1] = \mathbb{Q}[\beta_2] = K$ et que $M_\alpha = M_{\beta_1} + M_{\beta_2}$ et donc $Tr(M_\alpha) = Tr(M_{\beta_1}) + Tr(M_{\beta_2})$.
avec $Tr(M_{\beta_1}) = \sum_{i=1}^n \sigma_i(\beta_1)$ $\quad Tr(M_{\beta_2}) = \sum_{i=1}^n \sigma_i(\beta_2)$ on obtient

bien $Tr(M_\alpha) = \sum_{i=1}^n \sigma_i(\beta_1) + \sigma_i(\beta_2) = \sum_{i=1}^n \sigma_i(\alpha)$

9) $D(\alpha_1, \ldots, \alpha_n) = \text{dét}\left(\sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j)\right) = \text{dét}\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right)$

Si on considère la matrice $S_\alpha = (\sigma_i(\alpha_j))_{\substack{1\le i\le n\\ 1\le j\le n}}$ on aura

$D(\alpha_1, \ldots, \alpha_n) = \text{dét}({}^tS_\alpha S_\alpha) = \text{dét}({}^tS_\alpha)\ \text{dét}(S_\alpha) = \det(S_\alpha)^2 = (\text{dét}(\sigma_i(\alpha_j)))^2$

10) On a $\sigma_i(\beta_j) = \sum_{p=1}^{n} \sigma_i(\alpha_p) A_{j,p}$ (car $A_{j,p} \in \mathbb{Q}$)

donc $S_\beta = S_\alpha\, {}^tA$ et $\det S_\beta = (\text{dét}\, S_\alpha)(\text{dét}\, A)$

On aura bien $D(\beta_1, \ldots, \beta_n) = (\det A)^2 D(\alpha_1, \ldots, \alpha_n)$

11) $D(1, \theta, \ldots, \theta^{n-1})$ ~~est le déterminant~~ vaut $(V(\sigma_1(\theta), \ldots, \sigma_n(\theta)))^2$

où $V(\sigma_1(\theta), \ldots, \sigma_n(\theta))$ est le déterminant de Vandermonde.

$$D(1, \theta, \ldots, \theta^{n-1}) = \left(\prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))\right)^2$$

Or $\prod_{i>j}(\sigma_i(\theta) - \sigma_j(\theta)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))$

et finalement $D(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\sigma_i(\theta) - \sigma_j(\theta))$

12) $(1, \theta, \ldots, \theta^{n-1})$ est une $\mathbb{Q}$-base de K, on peut donc

écrire $\forall i \quad \alpha_i = \sum_{p=1}^{n} A_{i,p}\, \theta^p \quad (A_{i,p} \in \mathbb{Q})$. et

$(\alpha_1, \ldots, \alpha_n)$ est une base de K ssi A est inversible.

Or $D(\alpha_1, \ldots, \alpha_n) = (\det A)^2 D(1, \ldots, \theta^{n-1})$ et $D(1, \ldots, \theta^{n-1}) \neq 0$

car les $\sigma_i(\theta)$ sont distincts, par conséquent :

$(\alpha_1, \ldots, \alpha_n)$ est une $\mathbb{Q}$-base de ~~K~~ ssi $D(\alpha_1, \ldots, \alpha_n) \neq 0$.

13) a) L'étude de $f : x \mapsto x^3 - x - 1$, avec $f'(x) = 3x^2 - 1$ est résumée dans le tableau de variations :

x	$-\infty$		$-\frac{1}{\sqrt{3}}$		$\frac{1}{\sqrt{3}}$		$+\infty$
f		$\nearrow$	$\frac{2}{3\sqrt{3}} - 1 < 0$	$\searrow$	$-\frac{2}{\sqrt{3}} - 1$	$\nearrow$	$+\infty$

le théorème de la bijection montre qu'elle possède un unique zéro, appartenant à $]\frac{1}{\sqrt{3}}, +\infty[$.

13.b) $P = X^3 - X - 1$ annule θ. Il est irréductible sur $\mathbb{Q}$ (9)

(Sinon il posséderait un facteur de degré 1, donc une racine rationnelle qui ne pourrait être que 1 ou -1 (idem 2.b) ce qui n'est pas le cas).

On a donc $P_{\mathbb{Q}}(\theta) = X^3 - X - 1$.

13.c) $D(1, \theta, \theta^2) = (-1)^{\frac{3\times 2}{2}} \prod_{i \neq j} (\theta_i - \theta_j)$ où θ_1, θ_2 et θ_3 sont les racines complexes de $P_{\mathbb{Q}}(\theta)$.

$P_{\mathbb{Q}}(\theta) = \prod_{j=1}^{3} (X - \theta_j)$ $\quad P'_{\mathbb{Q}}(\theta) = \sum_{k=1}^{3} \prod_{j \neq k} (X - \theta_j)$.

donc $P'_{\mathbb{Q}}(\theta_i) = \prod_{j \neq i} (\theta_i - \theta_j)$ et finalement

$$D(1, \theta, \theta^2) = - \prod_{i=1}^{3} P'(\theta_i) = -(3\theta_1^2 - 1)(3\theta_2^2 - 1)(3\theta_3^2 - 1)$$
$$= -\left[27(\theta_1\theta_2\theta_3)^2 - 9(\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + (\theta_2\theta_3)^2) + 3(\theta_1^2 + \theta_2^2 + \theta_3^2) - 1\right]$$

Or $\theta_1\theta_2\theta_3 = -(-1) = 1$ $\quad \theta_1^2\theta_2^2 + (\theta_1\theta_3)^2 + (\theta_2\theta_3)^2 = (\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1)^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3)$

$$\theta_1^2\theta_2^2 + (\theta_1\theta_3)^2 + (\theta_2\theta_3)^2 = (-1)^2 - 2(1)(0) = 1$$

$$\theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) = 0^2 - 2(-1) = 2$$

Finalement

$$D(1, \theta, \theta^2) = -\left[27 - 9 + 6 - 1\right] = -23$$